



Amazon FSX für NetApp ONTAP

Trident

NetApp
February 02, 2026

Inhalt

Amazon FSX für NetApp ONTAP	1
Verwenden Sie Trident mit Amazon FSX für NetApp ONTAP	1
Anforderungen	1
Überlegungen	1
Authentifizierung	2
Getestete Amazon Machine Images (Amis)	3
Weitere Informationen	3
IAM-Rolle und AWS Secret erstellen	3
Erstellen Sie den AWS Secrets Manager Secret	4
IAM-Richtlinie erstellen	4
Installation Von Trident	9
Trident über Helm installieren	9
Installieren Sie Trident über das EKS-Add-on	11
Konfigurieren Sie das Speicher-Back-End	17
Integration von ONTAP-SAN- und NAS-Treibern	17
FSX für ONTAP-Treiber Details	19
Erweiterte Back-End-Konfiguration und Beispiele	20
Back-End-Konfigurationsoptionen für die Bereitstellung von Volumes	24
Bereitstellung von SMB-Volumina	26
Konfigurieren Sie eine Storage-Klasse und PVC	26
Erstellen Sie eine Speicherklasse	26
Erstellen Sie die PVC	28
Trident-Attribute	30
Beispielanwendung bereitstellen	31
Konfigurieren Sie das Trident EKS-Add-on auf einem EKS-Cluster	32
Voraussetzungen	33
Schritte	33
Installieren/deinstallieren Sie das Trident EKS-Add-On über CLI	34

Amazon FSX für NetApp ONTAP

Verwenden Sie Trident mit Amazon FSX für NetApp ONTAP

"Amazon FSX für NetApp ONTAP" Ist ein vollständig gemanagter AWS Service, mit dem Kunden Filesysteme auf Basis des NetApp ONTAP Storage-Betriebssystems starten und ausführen können. Mit FSX für ONTAP können Sie bekannte NetApp Funktionen sowie die Performance und Administration nutzen und gleichzeitig die Einfachheit, Agilität, Sicherheit und Skalierbarkeit beim Speichern von Daten in AWS nutzen. FSX für ONTAP unterstützt ONTAP Dateisystemfunktionen und Administrations-APIs.

Die Integration des Filesystems Amazon FSX for NetApp ONTAP mit Trident stellt sicher, dass Kubernetes-Cluster, die in Amazon Elastic Kubernetes Service (EKS) ausgeführt werden, persistente Block- und dateibasierte Volumes mit ONTAP bereitstellen können.

Ein Dateisystem ist die primäre Ressource in Amazon FSX, analog zu einem ONTAP-Cluster vor Ort. Innerhalb jeder SVM können Sie ein oder mehrere Volumes erstellen, bei denen es sich um Daten-Container handelt, die die Dateien und Ordner im Filesystem speichern. Mit Amazon FSX für NetApp ONTAP wird als gemanagtes Dateisystem in der Cloud zur Verfügung gestellt. Der neue Dateisystemtyp heißt **NetApp ONTAP**.

Durch den Einsatz von Trident mit Amazon FSX for NetApp ONTAP können Sie sicherstellen, dass Kubernetes-Cluster, die im Amazon Elastic Kubernetes Service (EKS) ausgeführt werden, persistente Block- und dateibasierte Volumes bereitstellen können, die von ONTAP unterstützt werden.

Anforderungen

"Trident-Anforderungen erfüllt" Um FSX for ONTAP mit Trident zu integrieren, benötigen Sie zusätzlich:

- Ein vorhandener Amazon EKS-Cluster oder selbst verwalteter Kubernetes-Cluster mit `kubectl` installiert.
- Ein vorhandenes Amazon FSX for NetApp ONTAP-Filesystem und eine Storage Virtual Machine (SVM), die über die Worker-Nodes Ihres Clusters erreichbar ist.
- Worker-Nodes, die vorbereitet sind "[NFS oder iSCSI](#)".



Achten Sie darauf, dass Sie die für Amazon Linux und Ubuntu erforderlichen Schritte zur Knotenvorbereitung befolgen "[Amazon Machine Images](#)" (Amis) je nach EKS AMI-Typ.

Überlegungen

- SMB Volumes:
 - SMB Volumes werden mit unterstützt `ontap-nas` Nur Treiber.
 - SMB-Volumes werden vom Trident EKS Add-on nicht unterstützt.
 - Trident unterstützt nur SMB Volumes, die in Pods gemountet sind, die nur auf Windows Nodes ausgeführt werden. Weitere Informationen finden Sie unter "["Vorbereitung zur Bereitstellung von SMB Volumes"](#)".
- Vor Trident 24.02 konnten auf Amazon FSX-Dateisystemen erstellte Volumes, bei denen automatische Backups aktiviert sind, von Trident nicht gelöscht werden. Um dieses Problem in Trident 24.02 oder höher zu vermeiden, geben Sie `apikey` in der Backend-Konfigurationsdatei für AWS FSX für ONTAP , AWS

apiRegion und AWS secretKey an fsxFilesystemID.



Wenn Sie eine IAM-Rolle als Trident angeben, können Sie die Felder `apiKey` und `secretKey` explizit als Trident auslassen `apiRegion`. Weitere Informationen finden Sie unter ["FSX für ONTAP Konfigurationsoptionen und Beispiele"](#).

Gleichzeitige Nutzung von Trident SAN/iSCSI und EBS-CSI-Treiber

Wenn Sie Ontap-San-Treiber (z. B. iSCSI) mit AWS (EKS, ROSA, EC2 oder einer anderen Instanz) verwenden möchten, kann es bei der auf den Knoten erforderlichen Multipath-Konfiguration zu Konflikten mit dem CSI-Treiber von Amazon Elastic Block Store (EBS) kommen. Um sicherzustellen, dass Multipathing funktioniert, ohne EBS-Festplatten auf demselben Knoten zu beeinträchtigen, müssen Sie EBS aus Ihrem Multipathing-Setup ausschließen. Dieses Beispiel zeigt eine `multipath.conf` Datei, die die erforderlichen Trident Einstellungen enthält und gleichzeitig EBS-Festplatten vom Multipathing ausschließt:

```
defaults {
    find_multipaths no
}
blacklist {
    device {
        vendor "NVME"
        product "Amazon Elastic Block Store"
    }
}
```

Authentifizierung

Trident bietet zwei Authentifizierungsmodi.

- Anmeldeinformationsbasiert (empfohlen): Speichert Anmeldeinformationen sicher in AWS Secrets Manager. Sie können den Benutzer für Ihr Dateisystem oder den für Ihre SVM konfigurierten Benutzer verwenden `fsxadmin` `vsadmin`.



Trident wird voraussichtlich als SVM-Benutzer oder als Benutzer mit einem anderen Namen, der dieselbe Rolle hat, ausgeführt `vsadmin`. Amazon FSX for NetApp ONTAP hat einen `fsxadmin` Benutzer, der den ONTAP-Cluster-Benutzer nur eingeschränkt ersetzt `admin`. Wir empfehlen die Verwendung `vsadmin` mit Trident.

- Zertifikat-basiert: Trident kommuniziert über ein auf Ihrer SVM installiertes Zertifikat mit der SVM auf Ihrem FSX Filesystem.

Weitere Informationen zur Aktivierung der Authentifizierung finden Sie in der Authentifizierung für Ihren Treibertyp:

- ["ONTAP NAS-Authentifizierung"](#)
- ["ONTAP SAN-Authentifizierung"](#)

Getestete Amazon Machine Images (Amis)

Der EKS Cluster unterstützt zwar verschiedene Betriebssysteme, AWS hat jedoch bestimmte Amazon Machine Images (Amis) für Container und EKS optimiert. Die folgenden AMIs wurden mit NetApp Trident 25.02 getestet.

AMI	NAS	NAS-Wirtschaftlichkeit	iSCSI	iSCSI-Economy
AL2023_x86_64_STANDARD	Ja.	Ja.	Ja.	Ja.
AL2_x86_64	Ja.	Ja.	Ja*	Ja*
BOTTLEROCKET_x86_64	Ja**	Ja.	K. A.	K. A.
AL2023_ARM_64_STANDARD	Ja.	Ja.	Ja.	Ja.
AL2_ARM_64	Ja.	Ja.	Ja*	Ja*
BOTTLEROCKET_ARM_64	Ja**	Ja.	K. A.	K. A.

- * Das Löschen des PV ist ohne Neustart des Knotens nicht möglich

- ** Funktioniert nicht mit NFSv3 mit Trident Version 25.02.



Wenn Ihr gewünschtes AMI hier nicht aufgeführt ist, bedeutet dies nicht, dass es nicht unterstützt wird, sondern dass es einfach nicht getestet wurde. Diese Liste dient als Leitfaden für AMIs, von denen bekannt ist, dass sie funktionieren.

Tests durchgeführt mit:

- EKS-Version: 1.32
- Installationsmethode: Helm 25.06 und als AWS-Add-On 25.06
- Für NAS wurden sowohl NFSv3 als auch NFSv4.1 getestet.
- Für SAN wurde nur iSCSI getestet, nicht NVMe-of.

Durchgeführte Tests:

- Erstellen: Storage-Klasse, pvc, POD
- Löschen: Pod, pvc (normal, qtree/lun – Economy, NAS mit AWS Backup)

Weitere Informationen

- ["Dokumentation zu Amazon FSX für NetApp ONTAP"](#)
- ["Blogbeitrag zu Amazon FSX für NetApp ONTAP"](#)

IAM-Rolle und AWS Secret erstellen

Sie können Kubernetes-Pods für den Zugriff auf AWS-Ressourcen konfigurieren, indem

Sie sich als AWS IAM-Rolle authentifizieren anstatt dafür explizite AWS-Anmelde Daten bereitstellen zu müssen.



Um sich mit einer AWS IAM-Rolle zu authentifizieren, müssen Sie über ein Kubernetes-Cluster mit EKS verfügen.

Erstellen Sie den AWS Secrets Manager Secret

Da Trident APIs gegen einen FSX vserver ausstellen wird, um den Speicher für Sie zu verwalten, benötigt es Anmeldeinformationen, um dies zu tun. Diese Zugangsdaten können Sie sicher über ein AWS Secrets Manager Secret übermitteln. Daher, wenn Sie noch nicht über eine, müssen Sie ein AWS Secrets Manager Secret, die die Anmeldeinformationen für das vsadmin-Konto erstellen.

Dieses Beispiel erstellt einen AWS Secret Manager Secret, um Trident CSI-Anmelde Daten zu speichern:

```
aws secretsmanager create-secret --name trident-secret --description  
"Trident CSI credentials"\  
--secret-string  
"{"username": "vsadmin", "password": "<svmpassword>"}"
```

IAM-Richtlinie erstellen

Für die korrekte Ausführung von Trident-Berechtigungen sind ebenfalls AWS-Berechtigungen erforderlich. Daher müssen Sie eine Richtlinie erstellen, die Trident die erforderlichen Berechtigungen erteilt.

In den folgenden Beispielen wird eine IAM-Richtlinie über die AWS-CLI erstellt:

```
aws iam create-policy --policy-name AmazonFSxNCSIDriverPolicy --policy  
-document file://policy.json  
--description "This policy grants access to Trident CSI to FSxN and  
Secrets manager"
```

JSON-Beispiel für Richtlinien:

```
{
  "Statement": [
    {
      "Action": [
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx>CreateVolume",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:UntagResource",
        "fsx:UpdateVolume",
        "fsx:TagResource",
        "fsx:DeleteVolume"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": "secretsmanager:GetSecretValue",
      "Effect": "Allow",
      "Resource": "arn:aws:secretsmanager:<aws-region>:<aws-account-id>:secret:<aws-secret-manager-name>*"
    }
  ],
  "Version": "2012-10-17"
}
```

Erstellen Sie eine Pod-Identität oder IAM-Rolle für die Dienstkontozuordnung (IRSA).

Sie können ein Kubernetes-Dienstkonto so konfigurieren, dass es eine AWS Identity and Access Management (IAM)-Rolle mit EKS-Pod-Identität oder eine IAM-Rolle für die Dienstkontozuordnung (IRSA) übernimmt. Alle Pods, die für die Verwendung des Dienstkontos konfiguriert sind, können dann auf alle AWS-Dienste zugreifen, für die die Rolle Zugriffsberechtigungen besitzt.

Pod-Identität

Amazon EKS Pod Identity-Zuordnungen bieten die Möglichkeit, Anmeldeinformationen für Ihre Anwendungen zu verwalten, ähnlich wie Amazon EC2-Instance-Profile Anmeldeinformationen für Amazon EC2-Instances bereitstellen.

Installieren Sie Pod Identity auf Ihrem EKS-Cluster:

Sie können die Pod-Identität über die AWS-Konsole oder mit dem folgenden AWS CLI-Befehl erstellen:

```
aws eks create-addon --cluster-name <EKS_CLUSTER_NAME> --addon-name eks-pod-identity-agent
```

Weitere Informationen finden Sie unter ["Einrichten des Amazon EKS Pod Identity Agent"](#) .

Erstellen Sie trust-relationship.json:

Erstellen Sie trust-relationship.json, damit der EKS-Dienstprinzipal diese Rolle für die Pod-Identität übernehmen kann. Erstellen Sie anschließend eine Rolle mit dieser Vertrauensrichtlinie:

```
aws iam create-role \
--role-name fsxn-csi-role --assume-role-policy-document file://trust-relationship.json \
--description "fsxn csi pod identity role"
```

trust-relationship.json-Datei:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "pods.eks.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ]
    }
  ]
}
```

Fügen Sie die Rollenrichtlinie der IAM-Rolle hinzu:

Fügen Sie die Rollenrichtlinie aus dem vorherigen Schritt an die erstellte IAM-Rolle an:

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:111122223333:policy/fsxn-csi-policy \
--role-name fsxn-csi-role
```

Erstellen Sie eine Pod-Identitätszuordnung:

Erstellen Sie eine Pod-Identitätszuordnung zwischen der IAM-Rolle und dem Trident-Dienstkontos (Trident-Controller).

```
aws eks create-pod-identity-association \
--cluster-name <EKS_CLUSTER_NAME> \
--role-arn arn:aws:iam::111122223333:role/fsxn-csi-role \
--namespace trident --service-account trident-controller
```

IAM-Rolle für die Dienstkontozuordnung (IRSA)

Verwenden der AWS CLI:

```
aws iam create-role --role-name AmazonEKS_FSxN_CSI_DriverRole \
--assume-role-policy-document file://trust-relationship.json
```

Trust-Relationship.json-Datei:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::<account_id>:oidc-provider/<oidc_provider>"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringEquals": {
          "<oidc_provider>:aud": "sts.amazonaws.com",
          "<oidc_provider>:sub": "system:serviceaccount:trident:trident-controller"
        }
      }
    }
  ]
}
```

Aktualisieren Sie die folgenden Werte in der `trust-relationship.json` Datei:

- **<account_id>** - Ihre AWS-Konto-ID
- **<oidc_provider>** - das OIDC Ihres EKS-Clusters. Sie können den `oidc_Provider` erhalten, indem Sie Folgendes ausführen:

```
aws eks describe-cluster --name my-cluster --query  
"cluster.identity.oidc.issuer"\  
--output text | sed -e "s/^https:\/\///"
```

Die IAM-Rolle mit der IAM-Richtlinie verknüpfen:

Nachdem die Rolle erstellt wurde, hängen Sie die Richtlinie (die im obigen Schritt erstellt wurde) mit diesem Befehl an die Rolle an:

```
aws iam attach-role-policy --role-name my-role --policy-arn <IAM policy  
ARN>
```

Verify OIDC Provider is associated:

Vergewissern Sie sich, dass der OIDC-Anbieter dem Cluster zugeordnet ist. Sie können sie mit diesem Befehl überprüfen:

```
aws iam list-open-id-connect-providers | grep $oidc_id | cut -d "/" -f4
```

Wenn die Ausgabe leer ist, weisen Sie IAM OIDC mit dem folgenden Befehl dem Cluster zu:

```
eksctl utils associate-iam-oidc-provider --cluster $cluster_name  
--approve
```

Wenn Sie eksctl verwenden, verwenden Sie das folgende Beispiel, um eine IAM-Rolle für ein Dienstkonto in EKS zu erstellen:

```
eksctl create iamserviceaccount --name trident-controller --namespace  
trident \  
--cluster <my-cluster> --role-name AmazonEKS_FSxN_CSI_DriverRole  
--role-only \  
--attach-policy-arn <IAM-Policy ARN> --approve
```

Installation Von Trident

Trident optimiert das Amazon FSX für NetApp ONTAP Storage-Management in Kubernetes, damit sich Ihre Entwickler und Administratoren voll und ganz auf den Applikationseinsatz konzentrieren können.

Sie können Trident mit einer der folgenden Methoden installieren:

- Helm
- EKS-Add-on

Wenn Sie die Snapshot-Funktionalität nutzen möchten, installieren Sie das Add-On für den CSI-Snapshot-Controller. Weitere Informationen finden Sie unter "["Snapshot-Funktionalität für CSI-Volumes aktivieren"](#) .

Trident über Helm installieren

Pod-Identität

1. Trident Helm Repository hinzufügen:

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

2. Installieren Sie Trident anhand des folgenden Beispiels:

```
helm install trident-operator netapp-trident/trident-operator
--version 100.2502.1 --namespace trident --create-namespace
```

Mit dem Befehl können `helm list` Sie Installationsdetails wie Name, Namespace, Diagramm, Status, App-Version und Revisionsnummer überprüfen.

```
helm list -n trident
```

NAME	NAMESPACE	REVISION	UPDATED
STATUS	CHART		APP VERSION
trident-operator	trident	1	2024-10-14
14:31:22.463122 +0300 IDT	deployed		trident-operator-
100.2502.0	25.02.0		

Dienstkontozuordnung (IRSA)

1. Trident Helm Repository hinzufügen:

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

2. Legen Sie die Werte für **Cloud-Anbieter** und **Cloud-Identität** fest:

```
helm install trident-operator netapp-trident/trident-operator
--version 100.2502.1 \
--set cloudProvider="AWS" \
--set cloudIdentity="'eks.amazonaws.com/role-arn:
arn:aws:iam::<accountID>:role/<AmazonEKS_FSxN_CSI_DriverRole>'" \
--namespace trident \
--create-namespace
```

Mit dem Befehl können `helm list` Sie Installationsdetails wie Name, Namespace, Diagramm, Status, App-Version und Revisionsnummer überprüfen.

```
helm list -n trident
```

NAME	NAMESPACE	REVISION	UPDATED
STATUS	CHART		APP VERSION
trident-operator	trident	1	2024-10-14
14:31:22.463122 +0300 IDT	trident-operator-100.2510.0	deployed	trident-operator-100.2510.0
	25.10.0		

Wenn Sie iSCSI verwenden möchten, stellen Sie sicher, dass iSCSI auf Ihrem Client-Rechner aktiviert ist. Wenn Sie das AL2023 Worker Node OS verwenden, können Sie die Installation des iSCSI-Clients automatisieren, indem Sie den Parameter „node prep“ in der Helm-Installation hinzufügen:



```
helm install trident-operator netapp-trident/trident-operator
--version 100.2502.1 --namespace trident --create-namespace --
set nodePrep={iscsi}
```

Installieren Sie Trident über das EKS-Add-on

Das Trident EKS Add-on enthält die neuesten Sicherheitspatches und Bug Fixes. Es wurde von AWS für die Zusammenarbeit mit Amazon EKS validiert. Mit dem EKS-Add-on können Sie sicherstellen, dass Ihre Amazon EKS-Cluster sicher und stabil sind und den Arbeitsaufwand für die Installation, Konfiguration und Aktualisierung von Add-Ons verringern.

Voraussetzungen

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind, bevor Sie das Trident Add-on für AWS EKS konfigurieren:

- Ein Amazon EKS Cluster-Konto mit Add-on-Abonnement
- AWS Berechtigungen für den AWS Marketplace:
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- AMI-Typ: Amazon Linux 2 (AL2_x86_64) oder Amazon Linux 2 Arm(AL2_ARM_64)
- Knotentyp: AMD oder ARM
- Ein bestehendes Amazon FSX für NetApp ONTAP-Filesystem

Aktivieren Sie das Trident Add-on für AWS

Management-Konsole

1. Öffnen Sie die Amazon EKS Konsole unter <https://console.aws.amazon.com/eks/home#/clusters>.
2. Wählen Sie im linken Navigationsbereich **Cluster** aus.
3. Wählen Sie den Namen des Clusters aus, für den Sie das NetApp Trident-CSI-Add-On konfigurieren möchten.
4. Wählen Sie **Add-ons** und dann **Weitere Add-Ons**.
5. Führen Sie die folgenden Schritte aus, um das Add-on auszuwählen:
 - a. Scrollen Sie nach unten zum Abschnitt **AWS Marketplace-Add-ons** und geben Sie „Trident“ in das Suchfeld ein.
 - b. Aktivieren Sie das Kontrollkästchen in der oberen rechten Ecke des Felds „Trident by NetApp“.
 - c. Wählen Sie **Weiter**.
6. Gehen Sie auf der Seite **Ausgewählte Add-Ons konfigurieren**-Einstellungen wie folgt vor:



Überspringen Sie diese Schritte, wenn Sie die Pod Identity-Zuordnung verwenden.

- a. Wählen Sie die **Version** aus, die Sie verwenden möchten.
- b. Wenn Sie die IRSA-Authentifizierung verwenden, achten Sie darauf, die in den optionalen Konfigurationseinstellungen verfügbaren Konfigurationseinstellungen festzulegen:
 - Wählen Sie die **Version** aus, die Sie verwenden möchten.
 - Folgen Sie dem **Add-on-Konfigurationsschema** und setzen Sie den Parameter **configurationValues** im Abschnitt **Konfigurationswerte** auf die Rollen-ARN, die Sie im vorherigen Schritt erstellt haben (der Wert sollte das folgende Format haben):

```
{  
  "cloudIdentity": "'eks.amazonaws.com/role-arn: <role ARN>'",  
  "cloudProvider": "AWS"  
}
```

+

Wenn Sie für die Konfliktlösungsmethode Überschreiben auswählen, können eine oder mehrere Einstellungen für das vorhandene Add-On mit den Amazon EKS-Zusatzeinstellungen überschrieben werden. Wenn Sie diese Option nicht aktivieren und es einen Konflikt mit Ihren bestehenden Einstellungen gibt, schlägt der Vorgang fehl. Sie können die resultierende Fehlermeldung verwenden, um den Konflikt zu beheben. Bevor Sie diese Option auswählen, stellen Sie sicher, dass das Amazon EKS-Add-On keine Einstellungen verwaltet, die Sie selbst verwalten müssen.

7. Wählen Sie **Weiter**.
8. Wählen Sie auf der Seite **Überprüfen und Hinzufügen Erstellen**.

Nachdem die Installation des Add-ons abgeschlossen ist, wird das installierte Add-on angezeigt.

AWS CLI

1. Erstellen Sie die add-on.json Datei:

Verwenden Sie für die Pod-Identität das folgende Format:



Verwenden Sie die

```
{  
  "clusterName": "<eks-cluster>",  
  "addonName": "netapp_trident-operator",  
  "addonVersion": "v25.6.0-eksbuild.1",  
}
```

Verwenden Sie für die IRSA-Authentifizierung das folgende Format:

```
{  
  "clusterName": "<eks-cluster>",  
  "addonName": "netapp_trident-operator",  
  "addonVersion": "v25.6.0-eksbuild.1",  
  "serviceAccountRoleArn": "<role ARN>",  
  "configurationValues": {  
    "cloudIdentity": "'eks.amazonaws.com/role-arn: <role ARN>'",  
    "cloudProvider": "AWS"  
  }  
}
```



Ersetzen Sie <role ARN> diese durch die ARN der Rolle, die im vorherigen Schritt erstellt wurde.

2. Installieren Sie das Trident EKS-Add-on.

```
aws eks create-addon --cli-input-json file://add-on.json
```

Eksctl

Mit dem folgenden Beispielbefehl wird das Trident EKS Add-On installiert:

```
eksctl create addon --name netapp_trident-operator --cluster  
<cluster_name> --force
```

Aktualisieren Sie das Trident EKS-Add-On

Management-Konsole

1. Öffnen Sie die Amazon EKS Konsole <https://console.aws.amazon.com/eks/home#/clusters>.
2. Wählen Sie im linken Navigationsbereich **Cluster** aus.
3. Wählen Sie den Namen des Clusters aus, für den Sie das NetApp Trident-CSI-Add-On aktualisieren möchten.
4. Wählen Sie die Registerkarte **Add-ons**.
5. Wählen Sie **Trident by NetApp** und dann **Bearbeiten**.
6. Gehen Sie auf der Seite **Configure Trident by NetApp** wie folgt vor:
 - a. Wählen Sie die **Version** aus, die Sie verwenden möchten.
 - b. Erweitern Sie die **Optionale Konfigurationseinstellungen** und ändern Sie sie nach Bedarf.
 - c. Wählen Sie **Änderungen speichern**.

AWS CLI

Im folgenden Beispiel wird das EKS-Add-on aktualisiert:

```
aws eks update-addon --cluster-name <eks_cluster_name> --addon-name
netapp_trident-operator --addon-version v25.6.0-eksbuild.1 \
--service-account-role-arn <role-ARN> --resolve-conflict preserve \
--configuration-values "{\"cloudIdentity\":
\"'eks.amazonaws.com/role-arn: <role ARN>'\"}"
```

Eksctl

- Überprüfen Sie die aktuelle Version des FSxN Trident CSI-Add-ons. Ersetzen Sie `my-cluster` den Cluster-Namen.

```
eksctl get addon --name netapp_trident-operator --cluster my-cluster
```

Beispielausgabe:

NAME	VERSION	STATUS	ISSUES
IAMROLE	UPDATE AVAILABLE	CONFIGURATION VALUES	
netapp_trident-operator	v25.6.0-eksbuild.1	ACTIVE	0
	{"cloudIdentity": "'eks.amazonaws.com/role-arn: arn:aws:iam::139763910815:role/AmazonEKS_FSXN_CSI_DriverRole'"}		

- Aktualisieren Sie das Add-on auf die Version, die unter UPDATE zurückgegeben wurde, die in der Ausgabe des vorherigen Schritts VERFÜGBAR ist.

```
eksctl update addon --name netapp_trident-operator --version
v25.6.0-eksbuild.1 --cluster my-cluster --force
```

Wenn Sie die Option entfernen `--force` und eine der Amazon EKS-Zusatzeinstellungen mit Ihren vorhandenen Einstellungen in Konflikt steht, schlägt die Aktualisierung des Amazon EKS-Zusatzes fehl. Sie erhalten eine Fehlermeldung, um den Konflikt zu beheben. Bevor Sie diese Option angeben, stellen Sie sicher, dass das Amazon EKS-Add-On keine Einstellungen verwaltet, die Sie verwalten müssen, da diese Einstellungen mit dieser Option überschrieben werden. Weitere Informationen zu anderen Optionen für diese Einstellung finden Sie unter "[Add-Ons](#)". Weitere Informationen zum Field Management von Amazon EKS Kubernetes finden Sie unter "[Außendienstmanagement von Kubernetes](#)".

Deinstallieren Sie das Trident EKS-Add-On bzw. entfernen Sie es

Sie haben zwei Optionen zum Entfernen eines Amazon EKS-Add-ons:

- **Add-on-Software auf Ihrem Cluster beibehalten** – Diese Option entfernt die Amazon EKS-Verwaltung aller Einstellungen. Amazon EKS kann Sie auch nicht mehr über Updates informieren und das Amazon EKS-Add-On automatisch aktualisieren, nachdem Sie ein Update gestartet haben. Die Add-on-Software auf dem Cluster bleibt jedoch erhalten. Mit dieser Option wird das Add-On zu einer selbstverwalteten Installation anstatt zu einem Amazon EKS-Add-on. Bei dieser Option haben Add-on keine Ausfallzeiten. Behalten Sie die Option im Befehl bei `--preserve`, um das Add-on beizubehalten.
- **Entfernen Sie Add-on-Software komplett aus Ihrem Cluster** – NetApp empfiehlt, das Amazon EKS-Add-on nur dann aus Ihrem Cluster zu entfernen, wenn es keine Ressourcen auf Ihrem Cluster gibt, die davon abhängen. Entfernen Sie die `--preserve` Option aus dem `delete` Befehl, um das Add-On zu entfernen.



Wenn dem Add-On ein IAM-Konto zugeordnet ist, wird das IAM-Konto nicht entfernt.

Management-Konsole

1. Öffnen Sie die Amazon EKS Konsole unter <https://console.aws.amazon.com/eks/home#/clusters>.
2. Wählen Sie im linken Navigationsbereich **Cluster** aus.
3. Wählen Sie den Namen des Clusters aus, für den Sie das NetApp Trident CSI-Add-On entfernen möchten.
4. Wählen Sie die Registerkarte **Add-ons** und dann **Trident by NetApp**.*
5. Wählen Sie **Entfernen**.
6. Gehen Sie im Dialogfeld **Remove netapp_Trident-Operator confirmation** wie folgt vor:
 - a. Wenn Amazon EKS die Verwaltung der Einstellungen für das Add-On einstellen soll, wählen Sie **auf Cluster beibehalten** aus. Führen Sie diese Option aus, wenn Sie die Add-on-Software auf dem Cluster beibehalten möchten, damit Sie alle Einstellungen des Add-ons selbst verwalten können.
 - b. Geben Sie **netapp_Trident-Operator** ein.
 - c. Wählen Sie **Entfernen**.

AWS CLI

Ersetzen `my-cluster` Sie den Namen des Clusters, und führen Sie dann den folgenden Befehl aus.

```
aws eks delete-addon --cluster-name my-cluster --addon-name  
netapp_trident-operator --preserve
```

Eksctl

Mit dem folgenden Befehl wird das Trident EKS-Add-On deinstalliert:

```
eksctl delete addon --cluster K8s-arm --name netapp_trident-operator
```

Konfigurieren Sie das Speicher-Back-End

Integration von ONTAP-SAN- und NAS-Treibern

Um ein Storage-Backend zu erstellen, müssen Sie eine Konfigurationsdatei im JSON- oder YAML-Format erstellen. Die Datei muss den gewünschten Speichertyp (NAS oder SAN), das Dateisystem und die SVM angeben, von der sie abgerufen werden soll, und wie die Authentifizierung mit ihr durchgeführt werden soll. Im folgenden Beispiel wird gezeigt, wie NAS-basierter Storage definiert wird und wie ein AWS-Schlüssel zum Speichern der Zugangsdaten für die zu verwendende SVM verwendet wird:

YAML

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: tbc-ontap-nas
  svm: svm-name
  aws:
    fsxFilesystemID: fs-xxxxxxxxxx
  credentials:
    name: "arn:aws:secretsmanager:us-west-2:xxxxxxxx:secret:secret-
name"
    type: awsarn
```

JSON

```
{
  "apiVersion": "trident.netapp.io/v1",
  "kind": "TridentBackendConfig",
  "metadata": {
    "name": "backend-tbc-ontap-nas",
    "namespace": "trident"
  },
  "spec": {
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "tbc-ontap-nas",
    "svm": "svm-name",
    "aws": {
      "fsxFilesystemID": "fs-xxxxxxxxxx"
    },
    "managementLIF": null,
    "credentials": {
      "name": "arn:aws:secretsmanager:us-west-2:xxxxxxxx:secret:secret-
name",
      "type": "awsarn"
    }
  }
}
```

Führen Sie die folgenden Befehle aus, um die Trident-Backend-Konfiguration (TBC) zu erstellen und zu validieren:

- Erstellen Sie die Trident-Backend-Konfiguration (TBC) aus der yaml-Datei, und führen Sie den folgenden Befehl aus:

```
kubectl create -f backendconfig.yaml -n trident
```

```
tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-nas created
```

- Überprüfen Sie, ob die Trident-Backend-Konfiguration (TBC) erfolgreich erstellt wurde:

```
Kubectl get tbc -n trident
```

NAME	PHASE	STATUS	BACKEND NAME	BACKEND UUID
backend-tbc-ontap-nas	b9ff-f96d916ac5e9	Bound	tbc-ontap-nas	933e0071-66ce-4324-

FSX für ONTAP-Treiber Details

Sie können Trident mithilfe der folgenden Treiber in Amazon FSX for NetApp ONTAP integrieren:

- **ontap-san**: Jedes bereitgestellte PV ist eine LUN innerhalb seines eigenen Amazon FSX für NetApp ONTAP-Volumens. Empfohlen für Blocklagerung.
- **ontap-nas**: Jedes bereitgestellte PV ist ein vollständiges Amazon FSX für NetApp ONTAP Volumen. Für NFS und SMB empfohlen.
- **ontap-san-economy**: Jedes bereitgestellte PV ist eine LUN mit einer konfigurierbaren Anzahl an LUNs pro Amazon FSX für das NetApp ONTAP Volume.
- **ontap-nas-economy**: Jedes bereitgestellte PV ist ein qtree mit einer konfigurierbaren Anzahl von qtrees pro Amazon FSX für NetApp ONTAP Volume.
- **ontap-nas-flexgroup**: Jedes bereitgestellte PV ist ein vollständiger Amazon FSX für NetApp ONTAP FlexGroup Volume.

Informationen zum Treiber finden Sie unter "["NAS-Treiber"](#) Und "["SAN-Treiber"](#)".

Nachdem die Konfigurationsdatei erstellt wurde, führen Sie diesen Befehl aus, um sie in Ihrem EKS zu erstellen:

```
kubectl create -f configuration_file
```

Führen Sie den folgenden Befehl aus, um den Status zu überprüfen:

```
kubectl get tbc -n trident
```

NAME	BACKEND NAME	BACKEND UUID
PHASE	STATUS	
backend-fsx-ontap-nas	backend-fsx-ontap-nas	7a551921-997c-4c37-a1d1-f2f4c87fa629
Bound	Success	

Erweiterte Back-End-Konfiguration und Beispiele

Die Back-End-Konfigurationsoptionen finden Sie in der folgenden Tabelle:

Parameter	Beschreibung	Beispiel
version		Immer 1
storageDriverName	Name des Speichertreibers	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, ontap-san-economy
backendName	Benutzerdefinierter Name oder das Storage-Backend	Treibername + „_“ + DatenLIF
managementLIF	IP-Adresse eines Clusters oder einer SVM-Management-LIF Ein vollständig qualifizierter Domain-Name (FQDN) kann angegeben werden. Kann so eingestellt werden, dass IPv6-Adressen verwendet werden, wenn Trident mit dem IPv6-Flag installiert wurde. IPv6-Adressen müssen in eckigen Klammern definiert werden, z. B. [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Wenn Sie den im aws Feld angeben fsxFilesystemID, müssen Sie den nicht angeben managementLIF, da Trident die SVM-Informationen von AWS abrufft managementLIF. Daher müssen Sie die Anmelddaten für einen Benutzer unter der SVM (z. B. vsadmin) angeben, und der Benutzer muss über die Rolle verfügen vsadmin .	„10.0.0.1“, „[2001:1234:abcd::fefe]“

Parameter	Beschreibung	Beispiel
dataLIF	IP-Adresse des LIF-Protokolls. ONTAP NAS-Treiber: NetApp empfiehlt die Angabe der DatenLIF. Wenn nicht angegeben, ruft Trident die DatenLIFs von der SVM ab. Sie können einen vollständig qualifizierten Domänennamen (FQDN) angeben, der für die NFS-Mount-Vorgänge verwendet werden soll. Dadurch können Sie ein Round-Robin-DNS erstellen, um den Lastausgleich über mehrere DatenLIFs hinweg zu ermöglichen. Kann nach der Anfangseinstellung geändert werden. Siehe . ONTAP-SAN-Treiber: Geben Sie nicht für iSCSI an. Trident verwendet die selektive LUN-Zuordnung von ONTAP, um die iSCSI LIFs zu ermitteln, die für die Einrichtung einer Multi-Path-Sitzung erforderlich sind. Eine Warnung wird erzeugt, wenn dataLIF explizit definiert ist. Kann so eingestellt werden, dass IPv6-Adressen verwendet werden, wenn Trident mit dem IPv6-Flag installiert wurde. IPv6-Adressen müssen in eckigen Klammern definiert werden, z. B. [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].	
autoExportPolicy	Aktivieren Sie die automatische Erstellung von Exportrichtlinien und aktualisieren Sie [Boolean]. Mithilfe der autoExportPolicy Optionen und autoExportCIDRs kann Trident Exportrichtlinien automatisch managen.	false
autoExportCIDRs	Liste der CIDRs, nach denen die Node-IPs von Kubernetes gegen gefiltert werden sollen, wenn autoExportPolicy aktiviert ist. Mithilfe der autoExportPolicy Optionen und autoExportCIDRs kann Trident Exportrichtlinien automatisch managen.	„[„0.0.0.0/0“, „::/0“]“
labels	Satz willkürlicher JSON-formatierter Etiketten für Volumes	„“

Parameter	Beschreibung	Beispiel
clientCertificate	Base64-codierter Wert des Clientzertifikats. Wird für zertifikatbasierte Authentifizierung verwendet	“
clientPrivateKey	Base64-kodierte Wert des privaten Client-Schlüssels. Wird für zertifikatbasierte Authentifizierung verwendet	“
trustedCACertificate	Base64-kodierte Wert des vertrauenswürdigen CA-Zertifikats. Optional Wird für die zertifikatbasierte Authentifizierung verwendet.	“
username	Benutzername zum Herstellen einer Verbindung zum Cluster oder zur SVM. Wird für die Anmeldeinformationsbasierte Authentifizierung verwendet. Beispiel: Vsadmin.	
password	Passwort für die Verbindung mit dem Cluster oder der SVM Wird für die Anmeldeinformationsbasierte Authentifizierung verwendet.	
svm	Zu verwendende Storage Virtual Machine	Abgeleitet, wenn eine SVM Management LIF angegeben ist.
storagePrefix	Das Präfix wird beim Bereitstellen neuer Volumes in der SVM verwendet. Kann nach der Erstellung nicht geändert werden. Um diesen Parameter zu aktualisieren, müssen Sie ein neues Backend erstellen.	trident
limitAggregateUsage	Nicht für Amazon FSX für NetApp ONTAP angeben. Die angegebenen fsxadmin und vsadmin enthalten nicht die erforderlichen Berechtigungen, um die aggregierte Nutzung abzurufen und sie mit Trident zu begrenzen.	Verwenden Sie ihn nicht.

Parameter	Beschreibung	Beispiel
limitVolumeSize	Bereitstellung fehlgeschlagen, wenn die angeforderte Volume-Größe über diesem Wert liegt. Beschränkt darüber hinaus die maximale Größe der Volumes, die es über qtrees und LUNs verwaltet, und qtreesPerFlexvol ermöglicht die Anpassung der maximalen Anzahl von qtrees pro FlexVol volume	„ (nicht standardmäßig durchgesetzt)
lunsPerFlexvol	Die maximale Anzahl an LUNs pro FlexVol volume muss im Bereich [50, 200] liegen. Nur SAN	„100“
debugTraceFlags	Fehler-Flags bei der Fehlerbehebung beheben. Beispiel, {„API“:false, „method“:true} Verwenden Sie es nicht debugTraceFlags Es sei denn, Sie beheben Fehler und benötigen einen detaillierten Log Dump.	Null
nfsMountOptions	Kommagetrennte Liste von NFS-Mount-Optionen. Die Mount-Optionen für persistente Kubernetes-Volumes werden normalerweise in Storage-Klassen angegeben. Wenn jedoch keine Mount-Optionen in einer Storage-Klasse angegeben sind, verwendet Trident die Mount-Optionen, die in der Konfigurationsdatei des Storage-Backends angegeben sind. Wenn in der Storage-Klasse oder in der Konfigurationsdatei keine Mount-Optionen angegeben sind, legt Trident keine Mount-Optionen auf einem zugeordneten persistenten Volume fest.	„
nasType	Konfiguration der Erstellung von NFS- oder SMB-Volumes Die Optionen lauten nfs, smb, Oder Null. Muss auf eingestellt sein smb Für SMB-Volumes. Einstellung auf null setzt standardmäßig auf NFS-Volumes.	nfs
qtreesPerFlexvol	Maximale Qtrees pro FlexVol volume, muss im Bereich [50, 300] liegen	“200”

Parameter	Beschreibung	Beispiel
smbShare	Sie können eine der folgenden Optionen angeben: Den Namen einer SMB-Freigabe, die mit der Microsoft Verwaltungskonsole oder der ONTAP-CLI erstellt wurde, oder einen Namen, mit dem Trident die SMB-Freigabe erstellen kann. Dieser Parameter ist für Amazon FSX for ONTAP Back-Ends erforderlich.	smb-share
useREST	Boolescher Parameter zur Verwendung von ONTAP REST-APIs. Wenn auf festgelegt <code>true</code> , verwendet Trident ONTAP REST APIs, um mit dem Backend zu kommunizieren. Diese Funktion erfordert ONTAP 9.11.1 und höher. Darüber hinaus muss die verwendete ONTAP-Anmelderolle Zugriff auf die Anwendung haben <code>ontap</code> . Dies wird durch die vordefinierten <code>vsadmin</code> Rollen und <code>cluster-admin</code> erreicht.	false
aws	In der Konfigurationsdatei für AWS FSX für ONTAP können Sie Folgendes angeben: <ul style="list-style-type: none"> - <code>fsxFilesystemID</code>: Geben Sie die ID des AWS FSX Dateisystems an. - <code>apiRegion</code>: Name der AWS API-Region. - <code>apikey</code>: AWS API-Schlüssel. - <code>secretKey</code>: AWS geheimer Schlüssel. 	"" "" ""
credentials	Geben Sie die FSX SVM-Zugangsdaten an, die in AWS Secrets Manager gespeichert werden sollen. <ul style="list-style-type: none"> - <code>name</code>: Amazon Resource Name (ARN) des Geheimnisses, das die Zugangsdaten von SVM enthält. - <code>type</code>: Gesetzt auf <code>awsarn</code>. Weitere Informationen finden Sie unter "Erstellen Sie einen AWS Secrets Manager-Schlüssel" .	

Back-End-Konfigurationsoptionen für die Bereitstellung von Volumes

Sie können die Standardbereitstellung mit diesen Optionen im `steuern defaults` Abschnitt der Konfiguration. Ein Beispiel finden Sie unten in den Konfigurationsbeispielen.

Parameter	Beschreibung	Standard
spaceAllocation	Speicherplatzzuweisung für LUNs	true
spaceReserve	Modus für Speicherplatzreservierung; „none“ (Thin) oder „Volume“ (Thick)	none
snapshotPolicy	Die Snapshot-Richtlinie zu verwenden	none
qosPolicy	QoS-Richtliniengruppe zur Zuweisung für erstellte Volumes Wählen Sie eine der qosPolicy oder adaptiveQosPolicy pro Storage-Pool oder Backend. Für die Verwendung von QoS-Richtliniengruppen mit Trident ist ONTAP 9.8 oder höher erforderlich. Sie sollten eine nicht gemeinsam genutzte QoS-Richtliniengruppe verwenden und sicherstellen, dass die Richtliniengruppe auf jede Komponente einzeln angewendet wird. Eine Shared-QoS-Richtliniengruppe erzwingt die Obergrenze für den Gesamtdurchsatz aller Workloads.	“
adaptiveQosPolicy	Adaptive QoS-Richtliniengruppe mit Zuordnung für erstellte Volumes Wählen Sie eine der qosPolicy oder adaptiveQosPolicy pro Storage-Pool oder Backend. Nicht unterstützt durch ontap-nas-Ökonomie	“
snapshotReserve	Prozentsatz des für Snapshots reservierten Volumes „0“	Wenn snapshotPolicy none , else „
splitOnClone	Teilen Sie einen Klon bei der Erstellung von seinem übergeordneten Objekt auf	false
encryption	Aktivieren Sie NetApp Volume Encryption (NVE) auf dem neuen Volume, Standardeinstellung ist false. NVE muss im Cluster lizenziert und aktiviert sein, damit diese Option verwendet werden kann. Wenn auf dem Backend NAE aktiviert ist, wird jedes in Trident bereitgestellte Volume NAE aktiviert. Weitere Informationen finden Sie unter "Funktionsweise von Trident mit NVE und NAE" .	false

Parameter	Beschreibung	Standard
luksEncryption	Aktivieren Sie die LUKS-Verschlüsselung. Siehe "Linux Unified Key Setup (LUKS) verwenden" . Nur SAN	„“
tieringPolicy	Tiering-Richtlinie für die Nutzung none	
unixPermissions	Modus für neue Volumes. Leere leer für SMB Volumen.	„“
securityStyle	Sicherheitstyp für neue Volumes. NFS unterstützt mixed Und unix Sicherheitsstile. SMB unterstützt mixed Und ntfs Sicherheitsstile.	NFS-Standard ist unix. SMB-Standard ist ntfs.

Bereitstellung von SMB-Volumina

Sie können SMB-Volumes mithilfe von ... bereitstellen. ontap-nas Treiber. Bevor Sie fertigstellen [Integration von ONTAP-SAN- und NAS-Treibern](#) Führen Sie diese Schritte aus: ["Vorbereitung zur Bereitstellung von SMB Volumes"](#) Die

Konfigurieren Sie eine Storage-Klasse und PVC

Konfigurieren Sie ein Kubernetes StorageClass-Objekt und erstellen Sie die Storage-Klasse, um Trident anzuweisen, wie Volumes bereitgestellt werden. Erstellen Sie ein PersistentVolumeClaim (PVC), das die konfigurierte Kubernetes StorageClass verwendet, um Zugriff auf das PV anzufordern. Anschließend können Sie das PV an einem Pod montieren.

Erstellen Sie eine Speicherklasse

Konfigurieren Sie ein Kubernetes StorageClass-Objekt

Der ["Kubernetes StorageClass-Objekt"](#) Das Objekt identifiziert Trident als den für diese Klasse verwendeten Provisioner und weist Trident an, wie ein Volume bereitgestellt wird. Verwenden Sie dieses Beispiel, um die Speicherklasse für Volumes mit NFS einzurichten (die vollständige Liste der Attribute finden Sie im Abschnitt „Trident -Attribute“ weiter unten):

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-gold
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  provisioningType: "thin"
  snapshots: "true"
```

Verwenden Sie dieses Beispiel, um die Speicherklasse für Volumes mit iSCSI einzurichten:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-gold
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
  provisioningType: "thin"
  snapshots: "true"
```

Fügen Sie zum Bereitstellen von NFSv3 Volumes auf AWS Bottlerocket die erforderliche Storage-Klasse hinzu `mountOptions`:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-gold
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
mountOptions:
  - nfsvers=3
  - nolock
```

Einzelheiten zur Interaktion von Storage-Klassen mit den `PersistentVolumeClaim` Parametern und zur Steuerung, wie Trident Volumes provisioniert, finden Sie unter "[Kubernetes und Trident Objekte](#)".

Erstellen Sie eine Speicherklasse

Schritte

1. Verwenden Sie dieses Objekt von Kubernetes `kubectl` Um sie in Kubernetes zu erstellen.

```
kubectl create -f storage-class-ontapnas.yaml
```

2. Sie sollten nun eine **Basic-csi** Storage-Klasse sowohl in Kubernetes als auch in Trident sehen, und Trident hätte die Pools auf dem Backend entdeckt haben sollen.

```
kubectl get sc basic-csi
```

NAME	PROVISIONER	AGE
basic-csi	csi.trident.netapp.io	15h

Erstellen Sie die PVC

A "[PersistentVolumeClaim](#)" (PVC) ist eine Anforderung für den Zugriff auf das PersistentVolume auf dem Cluster.

Die PVC kann so konfiguriert werden, dass eine Speicherung einer bestimmten Größe oder eines bestimmten Zugriffsmodus angefordert wird. Mithilfe der zugehörigen StorageClass kann der Clusteradministrator mehr als die Größe des PersistentVolume und den Zugriffsmodus steuern, z. B. die Performance oder das Service-Level.

Nachdem Sie die PVC erstellt haben, können Sie das Volume in einem Pod einbinden.

Beispielmanifeste

PersistentVolumeClaim-Beispielmanifeste

Diese Beispiele zeigen grundlegende PVC-Konfigurationsoptionen.

PVC mit RWX-Zugang

Dieses Beispiel zeigt ein einfaches PVC mit RWX-Zugriff, das mit einer StorageClass namens verknüpft ist `basic-csi`.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-storage
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-gold
```

PVC mit iSCSI-Beispiel

Dieses Beispiel zeigt ein grundlegendes PVC für iSCSI mit RWO-Zugriff, das mit einer StorageClass namens `protection-gold`.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-san
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: protection-gold
```

PVC erstellen

Schritte

1. Erstellen Sie die PVC.

```
kubectl create -f pvc.yaml
```

2. Überprüfen Sie den PVC-Status.

```
kubectl get pvc
```

NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS	AGE
pvc-storage	Bound	pv-name	2Gi	RWO		5m

Einzelheiten zur Interaktion von Storage-Klassen mit den PersistentVolumeClaim Parametern und zur Steuerung, wie Trident Volumes provisioniert, finden Sie unter ["Kubernetes und Trident Objekte"](#).

Trident-Attribute

Diese Parameter bestimmen, welche in Trident gemanagten Storage Pools zur Bereitstellung von Volumes eines bestimmten Typs verwendet werden sollten.

Attribut	Typ	Werte	Angebot	Anfrage	Unterstützt von
Medien ¹	Zeichenfolge	hdd, Hybrid, ssd	Pool enthält Medien dieser Art. Beides bedeutet Hybrid	Medientyp angegeben	ontap-nas, ontap-nas-Economy, ontap-nas-Flexgroup, ontap-san, solidfire-san
Bereitstellungstyp	Zeichenfolge	Dünn, dick	Pool unterstützt diese Bereitstellungsmethode	Bereitstellungsmethode angegeben	Thick: All ONTAP; Thin: Alle ONTAP und solidfire-san
BackendType	Zeichenfolge	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, azure-netapp-files, ontap-san-economy	Pool gehört zu dieser Art von Backend	Back-End angegeben	Alle Treiber
Snapshots	bool	Richtig, falsch	Pool unterstützt Volumes mit Snapshots	Volume mit aktivierten Snapshots	ontap-nas, ontap-san, solidfire-san
Klone	bool	Richtig, falsch	Pool unterstützt das Klonen von Volumes	Volume mit aktivierten Klonen	ontap-nas, ontap-san, solidfire-san

Attribut	Typ	Werte	Angebot	Anfrage	Unterstützt von
Verschlüsselung	bool	Richtig, falsch	Pool unterstützt verschlüsselte Volumes	Volume mit aktivierter Verschlüsselung	ontap-nas, ontap-nas-Economy, ontap-nas-Flexgroups, ontap-san
IOPS	Int	Positive Ganzzahl	Pool kann IOPS in diesem Bereich garantieren	Volume hat diese IOPS garantiert	solidfire-san

¹: Nicht unterstützt von ONTAP Select-Systemen

Beispielanwendung bereitstellen

Wenn die Storage-Klasse und die PVC erstellt wurden, können Sie das PV an einem Pod mounten. In diesem Abschnitt werden der Beispielbefehl und die Konfiguration zum Anbinden des PV an einen Pod aufgeführt.

Schritte

1. Mounten Sie das Volume in einem Pod.

```
kubectl create -f pv-pod.yaml
```

Diese Beispiele zeigen grundlegende Konfigurationen zum Anbringen der PVC an einem POD:
Grundkonfiguration:

```

kind: Pod
apiVersion: v1
metadata:
  name: pv-pod
spec:
  volumes:
    - name: pv-storage
      persistentVolumeClaim:
        claimName: basic
  containers:
    - name: pv-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
      volumeMounts:
        - mountPath: "/my/mount/path"
          name: pv-storage

```



Sie können den Fortschritt mit überwachen `kubectl get pod --watch`.

2. Vergewissern Sie sich, dass das Volume auf gemountet ist `/my/mount/path`.

```
kubectl exec -it pv-pod -- df -h /my/mount/path
```

Filesystem	Size
Used Avail Use% Mounted on	
192.168.188.78:/trident_pvc_ae45ed05_3ace_4e7c_9080_d2a83ae03d06	1.1G
320K 1.0G 1% /my/mount/path	

Sie können den Pod jetzt löschen. Die Pod Applikation wird nicht mehr existieren, aber das Volume bleibt erhalten.

```
kubectl delete pod pv-pod
```

Konfigurieren Sie das Trident EKS-Add-on auf einem EKS-Cluster

NetApp Trident optimiert das Amazon FSX für NetApp ONTAP Storage-Management in Kubernetes, damit sich Ihre Entwickler und Administratoren voll und ganz auf den

Applikationseinsatz konzentrieren können. Das NetApp Trident EKS Add-on enthält die neuesten Sicherheitspatches und Bug Fixes. Es wurde von AWS für die Zusammenarbeit mit Amazon EKS validiert. Mit dem EKS-Add-on können Sie sicherstellen, dass Ihre Amazon EKS-Cluster sicher und stabil sind und den Arbeitsaufwand für die Installation, Konfiguration und Aktualisierung von Add-Ons verringern.

Voraussetzungen

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind, bevor Sie das Trident Add-on für AWS EKS konfigurieren:

- Ein Amazon EKS-Cluster-Konto mit Berechtigungen zum Arbeiten mit Add-ons. Siehe "[Amazon EKS-Add-ons](#)".
- AWS Berechtigungen für den AWS Marketplace:
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- AMI-Typ: Amazon Linux 2 (AL2_x86_64) oder Amazon Linux 2 Arm(AL2_ARM_64)
- Knotentyp: AMD oder ARM
- Ein bestehendes Amazon FSX für NetApp ONTAP-Filesystem

Schritte

1. Erstellen Sie unbedingt eine IAM-Rolle und einen AWS Secret, damit EKS-Pods auf AWS Ressourcen zugreifen können. Anweisungen hierzu finden Sie unter "[IAM-Rolle und AWS Secret erstellen](#)".
2. Navigieren Sie auf Ihrem EKS Kubernetes-Cluster zur Registerkarte **Add-ons**.
3. Gehen Sie zu **AWS Marketplace Add-ons** und wählen Sie die Kategorie *Storage*.
4. Suchen Sie **NetApp Trident** und aktivieren Sie das Kontrollkästchen für das Trident-Add-on, und klicken Sie auf **Weiter**.
5. Wählen Sie die gewünschte Version des Add-ons aus.
6. Konfigurieren Sie die erforderlichen Add-On-Einstellungen.
7. Wenn Sie IRSA (IAM-Rollen für Dienstkonten) verwenden, lesen Sie die zusätzlichen Konfigurationsschritte "[Hier](#)".
8. Wählen Sie **Erstellen**.
9. Überprüfen Sie, ob der Status des Add-ons *Active* lautet.
10. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Trident ordnungsgemäß auf dem Cluster installiert ist:

```
kubectl get pods -n trident
```

11. Setzen Sie die Einrichtung fort und konfigurieren Sie das Storage-Back-End. Weitere Informationen finden Sie unter "[Konfigurieren Sie das Speicher-Back-End](#)".

Installieren/deinstallieren Sie das Trident EKS-Add-On über CLI

Installieren Sie das NetApp Trident EKS-Add-On über CLI:

Der folgende Beispielbefehl installiert das Trident EKS-Add-on:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.0-eksbuild.1 (mit einer dedizierten Version)
```

Der folgende Beispielbefehl installiert das Trident EKS-Add-on Version 25.6.1:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.1-eksbuild.1 (mit einer dedizierten Version)
```

Der folgende Beispielbefehl installiert das Trident EKS-Add-on Version 25.6.2:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.2-eksbuild.1 (mit einer dedizierten Version)
```

Deinstallieren Sie das NetApp Trident EKS-Add-On über CLI:

Mit dem folgenden Befehl wird das Trident EKS-Add-On deinstalliert:

```
eksctl delete addon --cluster K8s-arm --name netapp_trident-operator
```

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.